Title	Webアプリケーションにおけるプライバシ保護のためのフィルタリングシステムの開発
Author(s)	川本, 淳平; 吉川, 正俊
Citation	電子情報通信学会第二種研究会資料 IEICE SIG Notes : Webインテリジェンスとインタラクション (2007): 75-76
Issue Date	2007-12
URL	http://hdl.handle.net/2433/148001
Right	copyright (c)2007 IEICE
Type	Journal Article
Textversion	publisher

社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

第二種研究会資料
IEICE SIG Notes
WI2-2007-59(2007.12)

Webアプリケーションにおけるプライバシ保護のためのフィルタリングシステムの開発

Development of A Privacy Protection System for Web Applications

川本 淳平　　吉川 正俊
Junpei KAWAMOTO　Masatoshi YOSHIKAWA
京都大学大学院情報学研究科社会情報学専攻
Department of Social Informatics, Graduate School of Informatics, Kyoto University

1. はじめに

近年クライアント端末が高性能化しブロードバンドネットワークが普及したことで，Google カレンダー [1] や Remember The Milk[2] に代表される Web アプリケーションが急速に広まっている．Web アプリケーションは，今までデスクトップアプリケーションとして提供されてきたサービスを，Web を介しブラウザ上で実現する．Web を利用することで Web アプリケーションは次の特徴を持っている．

1. データが Web サーバ上で管理されるため，わざわざ持ち運ぶ必要がない
2. Web に接続できる端末があれば，いつでもどこからでもアプリケーションを利用できる

これらにより，ユビキタス・コンピューティング環境において Web アプリケーションは有効なサービスであると言える．しかし同時に，Web アプリケーションを提供するアプリケーションサーバには次の問題も指摘されている．

- セキュリティに配慮したデータ管理を提供しない場合がある
- 収集したユーザデータを別の用途に利用することがある

こうしたことから，Web アプリケーションの利用により，プライバシ情報が漏洩してしまうことが危惧されている．そこで，Web アプリケーション利用におけるプライバシ問題に関して，ユーザデータに対するフィルタリングを行うことで，意図しないユーザデータの送信や表示を防ぐシステムについて提案する．

2. Web アプリケーションの問題点

Web アプリケーションは，Web サーバ上でサービスを提供し，ユーザは Web ブラウザをクライアントとしてそれらのサービスを利用する．こうしたクライアント・サーバ型のアプリケーションである Web アプリケーションにおける多くの処理は，利用者から物理的に離れたサーバ上で行われる．そのため，ユーザはアプリケーションの実行に必要なデータをサーバへ送信する必要がある．例えば，Web カレンダーを利用している場合，スケジュールデータ等はサーバへ送信しなければスケジュール管理を行うことはできない．こうしたユーザが直接入力するデータは，「明示的な送信データ」と言える．他の明示的な送信データの例をいくつか挙げると，

- インターネットショッピングにおける購入履歴情報
- 乗り換え案内検索における乗車及び降車駅情報
- ソーシャルブックマークにおけるブックマーク情報

などがある．

Web アプリケーションが利用するデータには，明示的な送信データ以外にもある．例えば，インターネットショッピングにおいて閲覧したが購入には至らなかったが商品情報や，Web ブックマークにおけるマーキングページの閲覧回数や閲覧時刻などである．これらはユーザの意図しない，または知らない所で Web アプリケーションにより収集され，「非明示的な収集データ」と呼ぶことができる．また，明示的な送信データと非明示的な収集データを組み合わせることで，別のユーザ情報が収集されることもある．例えば，スケジュールデータと乗り換え案内検索情報を組み合わせることで，ユーザの 1 日の行動を把握することができる．

これらのユーザデータは，Web アプリケーションをユーザ毎にパーソナライズするために利用され，アプリケーションをより便利なものにするために利用されている．しかし，収集データの種類や収集方法，利用方法によってはユーザにとって好ましく無い場合もある．すなわち，Web アプリケーションが収集するユーザデータには，次のような問題があると考えられる．

- どのようなデータを収集しているのかが明確で無い
- どのような用途に用いているのかが明確で無い
- ユーザがデータ収集を拒否できない場合がある

このため，Web アプリケーションが収集するユーザデータは，プライバシに関わる可能性があると言える．しかし，ユーザデータはサービスプロバイダが管理しており，一部の明示的な送信データ以外をユーザがコントロールすることは難しい．特に非明示的な収集データに関しては，データを収集されていることに気付いていないユーザも多い．従って，ユーザにとって次のような問題が発生している．

1. プライバシに関わるデータが不要な場面で表示されてしまう．
2. プライバシに関わるデータが別のサービスのために利用されてしまう．
3. データの種類によってはユーザの意思で削除できないことがある．
4. 収集データの中には注意深く管理されないものも

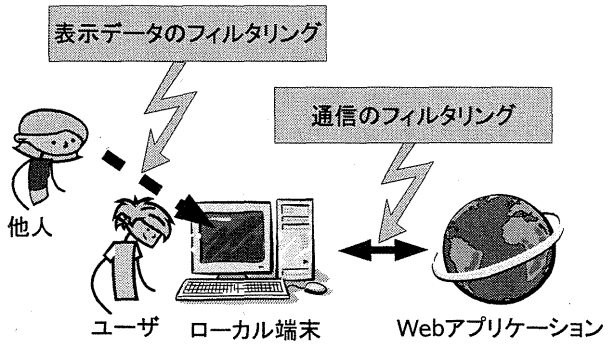

図 1: プライバシ・フィルタリングシステム

ある.

(1) は，例えば自宅以外や周囲に他人がいる状況で Web アプリケーションを利用した時に，インターネットショッピングの購入履歴やそれに基づく推薦商品が表示されてしまったり，プライベートなスケジュールが表示されてしまうということが挙げられる．(2) は，例えば広告表示に利用されたり，ソーシャルネットワーク・アプリケーションでは，似た興味を持つユーザの推薦に利用されたりすることが挙げられる．(3) は，例えば通院に関するスケジュールや乗換案内情報など，サービス利用時には必要な情報であったが，時間の経過と共に記録から削除した情報であっても，削除できない場合があることが挙げられる．(4) は，個人情報保護が叫ばれる近年，サービスプロバイダはユーザの個人情報に関係するデータは注意深く管理を行っていると言える．しかし，一般的には個人情報に該当しないが，ユーザによっては公開されることを嫌うデータもある．このようなデータに関しては，注意深く管理されないことがあることがある．

これらの問題は，データやユーザによっては気にならないこともある．しかし，深刻な問題へ発展する可能性もあり，我々は，ユーザ自身がプライバシコントロールを行える仕組みを提供する必要があると考えている．

3. 提案システム

本提案の目的は，前述の Web アプリケーションが収集するユーザデータに関するプライバシ問題を解決するために，ユーザに以下の機能を提供することである．

1. どの様なユーザデータがサービスプロバイダへ送信されているかを提示する．
2. ユーザが収集されるデータに関して，送信拒否を行える仕組みを提供する．
3. Web アプリが表示しようとするプライバシデータの表示をコントロールする．

(3) については，例えばコンテキスト毎にポリシを設定し，表示する内容を判別することを行う．本研究では，これらの機能をユーザに提供するために，図 1 に示す様なフィルタリングシステムの開発を行う．このフィルタリングシステムでは，プライバシ保護のために，通信のフィルタリングと表示データのフィルタリングという 2 種類のフィルタリングを行っている．

3.1 通信のフィルタリング

通信のフィルタリングでは，Web アプリケーションへ送信されるデータの中にプライバシに関わるデータが無いか調べるために，ローカル端末から Web アプリケーションへの通信を監視する．通信データにユーザが送信されることを望まないデータが含まれていた場合，次の 3 つの選択肢を提供する．

1. データの送信を遮断する
2. データを暗号化して送信する
3. セマンティックに基づくデータの置換を行う

(1) は最もセキュリティは高いが，送信を遮断してしまうと利用できないアプリケーションもある．(2) は暗号化はされているもののデータはサーバ上に保管されるため，上記 Web アプリケーションの特徴を損なうことなくプライバシを守ることができる．また，我々はサーバの送信データを暗号化した上で他のユーザとデータ共有を行うためのアクセス制御の導入方法について提案している [3]．本システムにおいてもこれらの技術を利用する．(3) のセマンティックに基づくデータの置換は，例えば「○○病院へ行く」と行った予定を抽象化し「外出」に置き換えるといったことを行う．

3.2 表示データのフィルタリング

表示データのフィルタリングでは，他人に見られたくないデータの表示を遮断する．表示に関するフィルタリングでは，「データの表示の遮断」と「セマンティックに基づくデータの置換」の 2 つの選択肢を提供する．

4. まとめ

本稿では，Web アプリケーションが利用するユーザデータと，それらに関するプライバシ問題について説明した．また，プライバシ問題を解決するためのシステムとして，開発中のフィルタリングソフトについて，その概要を説明した．今後は，提案システムを実装し効果を検証していく予定である．

参考文献

[1] Google カレンダー:
http://www.google.com/calendar/

[2] Remember The Milk:
http://www.rememberthemilk.com/

[3] 川本淳平, 吉川正俊, " データ共有型 Web アプリケーションにおけるサーバ暗号化, " データベースと Web 情報システムに関するシンポジウム (DBWeb2007), 2007 年 11 月.